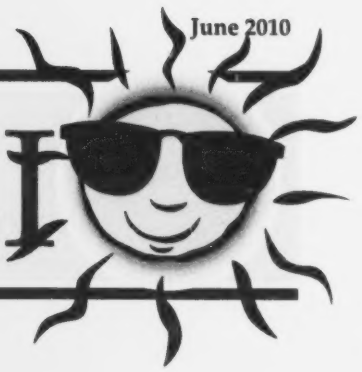
Office of the Saskatchewan Information and Privacy Commis- June 2010

FOIP FOLI



NOMINATIONS FOR CULLITON AWARD

This year, the Right to Know (RTK) steering committee is again seeking nominations for the *Chief Justice E.M. Culliton Right to Know Award*. Last year, the award was presented to **Dr. Robert McCulloch,** President and CEO of SIAST and **Sylvia Dycer,** FOIP Coordinator for SIAST. The intent of the award is to celebrate and to recognize leadership in promoting open and accountable government.

To be eligible, the body must be a Saskatchewan government institution (provincial government Ministry, Crown corporation, board, commission or agency) or a local authority (regional health authority, municipality, library, school, university or college).

The nominee should be an agency that has demonstrated some or all of the following qualities:

- Leadership in promoting public access to the agency's information;
- Creativity in building public awareness of access to information;
- Excellence in orientation of, and service training in, employee access to information responsibilities; and/or
- Innovation in the development of tools to promote or facilitate access to information.

The deadline for nominations is **September 15, 2010**. Nominations can be self-initiated or third party. The nomination should include:

- A letter of nomination (up to 1,000 words), and
- Samples of materials relevant to the nomination (testimonials or other material).

The award will be presented during Right to Know Week which will be held September 27-October 1, 2010. Nominations should be sent to the Right to Know Steering Committee, c/o #503, 1801 Hamilton Street, Regina, SK S4P 4B4 or fax (306) 798-1603 or email shickling@oipc.sk.ca

INSIDE THIS ISSUE

Nominations for Culliton Award.....1
SK Access, Privacy and Security Conference Set for September.....2
City of Saskatoon Privacy Breach.....2
OIPC 2009—2010 Annual Report.....2
Beware of Tabnapping.....3
AB Amends Private Sector Privacy Law.....3
Privacy Commissioner of Canada Annual Report.....3
SK Arbitrator Discounts Egregious Privacy Breach.....4
Cross-Border Data Flows and Privacy.....5
Mexico Passes Data Protection Law.....5
Amending PIPEDA.....5
BC OIPC Orders Insurance Corporation of British Columbia (ICBC) to Disclose "for Public Scrutiny Reasons".....6
FOIP and the Saskatchewan Legislative Assembly.....6
A Useful Paper on What is New in Privacy Law.....6
What is a Privacy Officer?.....6
No Requirement to Create Records.....7
Non-Profit Organizations should be Privacy Compliant.....7
Another Resource for Protecting Personal Health Information.....7

SASKATCHEWAN ACCESS, PRIVACY AND SECURITY CONFERENCE SET FOR SEPTEMBER

Duane Mombourquette, Executive Director of the Access and Privacy Branch in the Ministry of Justice and Attorney General is organizing a major conference for September 28 & 29, 2010. Mark this in your calendar today! You won't want to miss this program.

Tentatively, **Jennifer Stoddart** the Privacy Commissioner of Canada, **Frank Work** the Alberta Information and Privacy Commissioner and the Manitoba Ombudsman **Irene Hamilton** are scheduled to participate. More information for this conference to be held at the Regina Inn is available at www.justice.gov.sk.ca/accessandprivacy.

CITY OF SASKATOON PRIVACY BREACH

In late May, **Gary Dickson**, Saskatchewan Information and Privacy Commissioner (the Commissioner), issued his Investigation Report LA-2010-001. The Complainant, an employee of the City of Saskatoon (City) discovered that the City had disclosed her personal information to the Canada Revenue Agency (CRA), formerly Canada Customs and Revenue Agency. The Complainant asked the City what authority it had to disclose her personal information to CRA. When she did not receive a satisfactory answer, she raised her concerns with the Commissioner.

The Commissioner found that the City did not meet the burden of proof in showing that it had authority to disclose the Complainant's personal information pursuant to section 28(2)(h) of *The Local Authority Freedom of Information and Protection of Privacy Act* (LA FOIP). Furthermore, it did not show how utility information was required by the CRA for the purpose of administering or enforcing a tax law. The Commissioner also found that the City failed to exercise its discretion and disclosed more of the Complainant's personal information than necessary. As well, the Commissioner determined that the City did not respond adequately to the formal complaint. Finally, the Commissioner made several recommendations to the City for dealing with future requests for personal information from CRA. This Investigation Report is available at www.oipc.sk.ca under the *Reports* tab.

We encourage all public bodies who routinely disclose personal information to other government bodies to determine precisely what legal authority exists to do so and whether this is done consistent with privacy best practices.

OIPC 2009—2010 ANNUAL REPORT

Our latest Annual Report will be tabled with the Speaker of the Legislative Assembly on June 30, 2010. The Commissioner will speak about that Annual Report at a news conference on the same day. At the same time the Annual Report will be posted to our website www.oipc.sk.ca and a copy of the CD will be sent to all government institutions, local authorities and health regulatory bodies.

BEWARE OF TABNAPPING

Tabnapping is yet another threat to the security of Internet users. This involves phishers who con individuals into giving up passwords by covertly changing browser tabs that are already open. Users will revisit a tab and enter their username and password to log in again except this time they are disclosing their username and password to a tabnapper. This threat is facilitated by users who leave numerous tabs open for long periods. To avoid this hazard, if a log-in screen appears on a tab you haven't opened yourself, do not log in to that screen. If you see a tab on your screen that contains what appears to be an apparently normal log-in form, best to close it and then go the site yourself in a new tab. Another safeguard is to examine the URL in the address bar on your browser before filling in any form or sharing any of your personal information. If you are experiencing an attempted tabnapping you will notice that the URL won't match the trick log-in screen.

ALBERTA AMENDS PRIVATE SECTOR PRIVACY LAW

Effective May 1, 2010 changes came into force for the Alberta *Personal Information Protection Act*. This means more stringent privacy rules for private sector businesses in that province. This clarifies the rules for the personal information for employees of a business. It requires that a business destroys personal information once it no longer requires it for legal or legitimate business purposes. In terms of penalties, the qualification of "willful" has been eliminated so that an offence can occur even if the organization acted unintentionally. There is a requirement to notify individuals if their personal information is to be transferred to a foreign service provider and to notify the Alberta Information and Privacy Commissioner if personal information is lost, accessed or disclosed without authorization.

PRIVACY COMMISSIONER OF CANADA ANNUAL REPORT

Jennifer Stoddart, Privacy Commissioner of Canada, released her *Annual Report to Parliament 2009, Report on the Personal Information Protection and Electronic Documents Act* (PIPEDA) in June 2010.

The Privacy Commissioner discusses her collaborative work with the OIPC on a number of projects including the development of privacy tools for Saskatchewan credit unions and small businesses. This includes the following commentary from Commissioner Stoddart:

> *We have also launched some joint public education initiatives aimed at both individuals and organizations. In Saskatchewan, for example, we are working in partnership with our provincial counterpart to develop privacy tools for credit unions and small businesses, with a view to using the lessons learned in other provinces and territories. As part of this work, we, in partnership with the Saskatchewan Office of the Information and Privacy Commissioner, are developing a co-branded website to deliver content and interact with Saskatchewan credit unions and small-and medium-sized businesses.*

Saskatchewan's access and privacy community is encouraged to read this Annual Report as it considers many things including:

- increasing global nature of information flows
- international organization for standardization and international initiatives
- mortgage broker breaches and systemic privacy issues
- social networking, new technologies and

(Continued on page 4)

(Continued from page 3)

surveillance concerns
- new early resolution initiatives for case files
- data breach reporting
- a number of relevant court decisions

The Annual Report is available at www.priv.gc.ca.

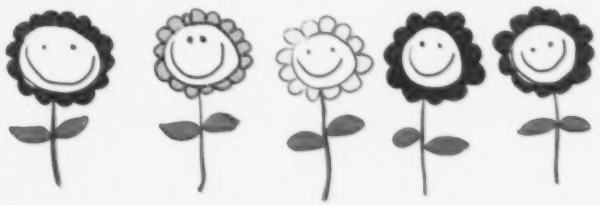
SASKATCHEWAN ARBITRATOR DISCOUNTS EGREGIOUS PRIVACY BREACH

On May 27, 2010, Mediator and Arbitrator **Catherine M. Zuck, Q.C.,** issued an award that overturned the dismissal for cause of a Saskatoon Regional Health Authority (RHA) employee who deliberately used computer equipment to view the personal health information (phi) of a third party in violation of her training, the privacy policy of the region and the Statement of Understanding on Confidentiality that the employee had signed. Arbitrator Zuck substituted only a 20 working day unpaid suspension. Remarkably, the employee worked in the Health Information Services office and had specific responsibility for training other staff on the Pharmaceutical Information Program (PIP) and the Enovation software program.

Enovation allows the user to collect a good deal of phi of patients in the RHA including name and registration information, the presenting health problem, treatment, physician, tests done and any hospital stays. The employee was accredited to enter both the PIP and the Enovation databases. To compound her privacy breach, the employee then disclosed information she had learned about the patient to another employee of the RHA who would have had no legitimate need to know that phi of the patient. Our OIPC is troubled by the decision and the underlying analysis. Much weight was apparently attached to the following findings of the Arbitrator:

- The employee's use of the patient's phi was not planned but was impulsive **[yet was clearly deliberate and not accidental]**
- She had no malicious intent **[not a requirement for a *The Health Information Protection Act* (HIPA) breach]**
- She didn't use the patient's phi for "personal gain" **[perhaps not financial but clearly it was information this employee searched for her own purposes i.e. not for the benefit of the patient. In any event this also is not a requirement for a HIPA breach.]**

Perhaps most surprising in this decision is not a single reference to the electronic health record which is the reason HIPA was enacted. There is no reference to the injury to the public's confidence that their privacy will be respected and their phi adequately protected in an E-health world. That includes protection from just this kind of inappropriate and illegal snooping. The OIPC will be meeting with Saskatchewan Health and Justice officials to consider strategies to ensure that any future privacy breaches will result in major penalties including dismissal.



CROSS-BORDER DATA FLOWS AND PRIVACY

The Hague Conference on Private International Law has adopted a document known as *Cross-Border Data Flows and Protection of Privacy.* The Hague Conference is an international organization based in the Netherlands that promotes inter-governmental coordination in the area of private international law. The document is useful as an excellent backgrounder on cross-border issues and the difficulty in assessing which law and which jurisdiction when dealing with cross-border data flows. Interestingly, the work on Canada's electronic health record raises many of the same types of issues that the Hague Conference is wrestling with at the international level. The document is available at http://www.hcch.net

MEXICO PASSES DATA PROTECTION LAW

Are you concerned that your credit card from that February winter break in Puerto Vallarta may have been used by identity thieves? Well, you now may have another resource in trying to figure out what happened and what you can do about it. In April, 2010 the Senate in Mexico enacted a data protection law that

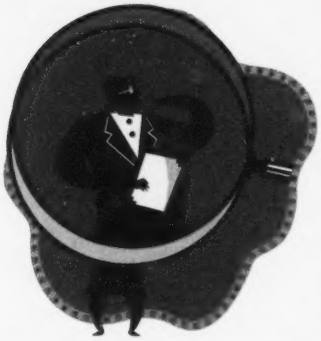
prescribes how private and public entities collect, use and disclose personal information of Mexicans. This also expands the jurisdiction of the Federal Institute of Access to Information and Data Protection to undertake privacy investigations. The website for the Institute is accessible at: www.ifai.org.mx.

AMENDING PIPEDA

The Government of Canada has introduced an amendment package for the *Personal Information Protection and Electronic Documents Act* (PIPEDA). These amendments reflect changes that follow a Parliamentary review of the law in 2009. The amendments include a mandatory breach reporting requirement and a broader exemption for business contact information. In addition, there is a new approach to consent for employee information (only for federal works, undertakings) and inclusion of 'work product'. These changes to the federal private sector privacy law reflect features in the British Columbia and Alberta legislation that have worked well for small and medium sized businesses. The mandatory breach notification requires an organization to report any material breach of security safeguards involving personal information under that organization's control. The amendments make it clear that the breach occurs when an organization fails to establish appropriate safeguards regardless of whether the personal information gets into the hands of a third party. More information is available at http://www.ic.gc.ca/eic/site/ecic-ceac.nsf/eng/h_gv00045.html.

Since PIPEDA applies to most Saskatchewan businesses and all organizations that collect, use or disclose personal information in the course of commercial activities it is advisable for those organizations to become familiar with the amendments and determine how they will affect their business operations. Just by way of reminder, PIPEDA will apply to the personal information of customers or clients of those businesses and organizations but does not apply to the personal information of their employees.

BC OIPC ORDERS INSURANCE CORPORATION OF BRITISH COLUMBIA (ICBC) TO DISCLOSE "FOR PUBLIC SCRUTINY REASONS"



The ICBC has been ordered by the Office of the British Columbia Information and Privacy Commissioner to release records related to termination of employees, severance paid and discipline imposed following an investigation by PricewaterhouseCoopers into ICBC's Material Damage Training and Research Facility. An affected third party requested a review of ICBC's decision to disclose severed records related to him. ICBC's proposed application of section 22 (disclosure harmful to personal privacy) found to be correct except for the amount of third party's severance which is ordered disclosed for public scrutiny reasons. Order F10-21 is available at http://www.oipc.bc.ca/Orders/2010/OrderF10-21.pdf.

FOIP AND THE SASKATCHEWAN LEGISLATIVE ASSEMBLY

There has been considerable interest in the issue of whether **Sheila Fraser**, Auditor General is entitled to audit the expenses of Members of Parliament. Related to this question is whether the Legislative Assembly Service and the offices of Members of the Legislative Assembly are subject to FOIP. The short answer is NO. The definition of "government institution" in section 2(2) of FOIP explicitly excludes the Legislative Assembly and the offices of Members. In a number of other provinces, the access and privacy legislation has been expanded to include the legislature administrative offices and all administrative expenses of MLA offices. In those provinces, one can make an access request for information for expenses paid for with public funds but cannot access the files that relate to particular constituents and their issues or complaints. Although one cannot submit a formal request for information under the FOIP Act, be aware that citizens can seek access directly through the individual constituency office of any MLA or through the office of the Clerk of the Legislative Assembly.

A USEFUL PAPER ON WHAT IS NEW IN PRIVACY LAW

Alex Cameron of the Toronto office of the law firm Fasken Martineau DuMoulin LLP presented an excellent paper at the April 2010 15th Biennial National Conference: New Developments in Communications Law and Policy. The paper is entitled *Facebook, Streetview and What's Next: Navigating Your Way Through New Issues in Privacy Law.* The paper can be downloaded at the website: http://www.fasken.com/new_issues_inprivacy_law/.

WHAT IS A PRIVACY OFFICER?

A useful tool developed by Service Alberta for purposes of that province's *Personal Information Protection Act* is entitled *What is a Privacy Officer?* This two page document may be useful for any organizations that are still in the process of tasking privacy

responsibility to someone in their organization. This is available at http://pipa.alberta.ca.

NO REQUIREMENT TO CREATE RECORDS

Michael McEvoy, Adjudicator in the BC Information and Privacy Commissioner Office, determined that the Ministry of Finance in that province was not required to create the records at issue in the inquiry. Two journalists had requested records in an electronic format containing the names of government employees along with their salary expenses, job title and department. The Ministry had replied that the record could not be created from a machine readable record in its custody or control using its normal hardware and software and technical expertise. Order F10-16 is available at http://www.oipc.bc.ca/orders/2010/OrderF10-16.pdf

NON-PROFIT ORGANIZATIONS SHOULD BE PRIVACY COMPLIANT

Our office often receives calls and inquiries from Saskatchewan residents about non-profit organizations and what obligations they have to protect personal information. As it stands, non-profit organizations are not covered by any of Canada's or Saskatchewan's major privacy laws. This should be qualified in two ways: (1) If the non-profit organization carries on a commercial activity (fundraising doesn't count as commercial activity) then the federal private sector PIPEDA law may apply. (2) If the non-profit organization does fee for service work for a Saskatchewan government institution or local authority, it may have in its possession certain records or personal information that would be "in the control" of that government institution or local authority.

We discuss these issues in our pamphlet, *A Contractor's Guide to Access and Privacy in Saskatchewan* available on our website: www.oipc.sk.ca.

Nonetheless, the *Personal Information Protection Act* in British Columbia and Alberta does apply to non-profits. Since Saskatchewan non-profits do depend on public goodwill and public confidence, it makes good sense that they try to model privacy best practices. We often encourage non-profits to consider some of the materials produced by the two far western provinces that may give them good ideas of what they could do to develop appropriate policies. In particular, we'd encourage our non-profits to consider a new publication from the Service Alberta entitled *Protecting Personal Information, A Workbook for Non-Profit Organizations.* This includes a sample privacy policy, a sample privacy statement and a list of other useful resources. This can be found at http://www.pipa.alberta.ca/nonprofits/pdf/npworkbook.pdf

ANOTHER RESOURCE FOR PROTECTING PERSONAL HEALTH INFORMATION

In the United States, the *Health Insurance Portability and Accountability Act* (HIPAA) requires the establishment of national standards for electronic health care transactions and national identifiers for providers, health insurance plans and employers. Part of the HIPAA apparatus is a *Privacy Rule* and a *Security Rule*. Despite the many differences between the U.S. health care system and our system in Saskatchewan, there is some useful material related to the *Security Rule* standards. A good example is a new instrument: *HIPAA Security Standards: Guidance on Risk Analysis*. This and other instruments are available at the website: http://www.hhs.gov/ocr/hipaa. Trustees are, of course, encouraged to become familiar with the COACH (Canada's Health Informatics Association) standards and these US materials should only be viewed as a supplementary resource.

MARK YOUR CALENDAR!

September 15, 2010: *Deadline for Culliton Award nominations.* Nominations should be sent to the Right to Know Steering Committee, c/o #503, 1801 Hamilton Street, Regina, SK S4P 4B4 or fax (306) 798-1603 or email shickling@oipc.sk.ca

September 19—20, 2010: *CBA National Privacy and Access Law Conference, "Privacy and Access Rights in the Age of Technology: the State of Canadians' Information Rights in 2010 and Beyond"*, Ottawa, Ontario. For more information, visit http://www.cba.org/pd/details.aspx?id=NA_PRV10

September 27—29, 2010: *Saskatchewan Access, Privacy, Security and Records Management Forum 2010—"Making Connections"*, Regina Inn, Regina, Saskatchewan. For more information, visit www.verney.ca/sk2010

September 28, 2010: *"Right to Know"* reception will be held in conjunction with the Saskatchewan Access, Privacy, Security and Records Management Forum 2010 noted above. Stay tuned for more details.

November 2—3, 2010: *PIPA Conference 2010—"Getting Through the Privacy Jungle—How to See the Forest...and the Trees"*. For more information, visit http://www.privacyconference.ca/agenda.php

Have a great summer!

OFFICE OF THE SASKATCHEWAN INFORMATION AND PRIVACY COMMISSIONER

503 – 1801 Hamilton Street
Regina, Saskatchewan
S4P 4B4

Telephone: (306) 787-8350 / Toll Free: 1-877-748-2298
Fax: (306) 798-1603
E-mail: webmaster@oipc.sk.ca

Website: www.oipc.sk.ca

If you wish to subscribe to the Saskatchewan FOIP FOLIO, please send your